

dry, and we are taking steps to ensure water for our future.

The City and the Bureau of Reclamation have already advanced the project by completing a favorable Appraisal Report and beginning a Feasibility Study. The Appraisal Report concluded that the city's projected water "shortage can be eliminated by more aggressive water reclamation" and that "there is a Federal interest in pursuing water reclamation and reuse investigations in Austin."

In 1907, Theodore Roosevelt said, "The conservation of natural resources is the fundamental problem. Unless we solve that problem, it will avail us little to solve all others." With your help, the capital of the Lone Star State can make even more significant strides in managing its water resources. I urge approval of this legislation.

Mrs. CHRISTENSEN. Madam Speaker, I yield back the balance of my time.

Mr. RENZI. Madam Speaker, I appreciate the leadership of the gentleman from Texas, and I yield back the balance of my time.

The SPEAKER pro tempore. The question is on the motion offered by the gentleman from Arizona (Mr. RENZI) that the House suspend the rules and pass the bill, H.R. 2341, as amended.

The question was taken; and (two-thirds having voted in favor thereof) the rules were suspended and the bill, as amended, was passed.

A motion to reconsider was laid on the table.

## TELEPHONE RECORDS AND PRIVACY PROTECTION ACT OF 2006

Mr. SENSENBRENNER. Madam Speaker, I move to suspend the rules and pass the bill (H.R. 4709) to amend title 18, United States Code, to strengthen protections for law enforcement officers and the public by providing criminal penalties for the fraudulent acquisition or unauthorized disclosure of phone records, as amended.

The Clerk read as follows:

H.R. 4709

*Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,*

### SECTION 1. SHORT TITLE.

This Act may be cited as the "Telephone Records and Privacy Protection Act of 2006".

### SEC. 2. FINDINGS.

Congress finds that—

(1) telephone records can be of great use to criminals because the information contained in call logs may include a wealth of personal data;

(2) call logs may reveal the names of telephone users' doctors, public and private relationships, business associates, and more;

(3) call logs are typically maintained for the exclusive use of phone companies, their authorized agents, and authorized consumers;

(4) telephone records have been obtained without the knowledge or consent of consumers through the use of a number of fraudulent methods and devices that include—

(A) telephone company employees selling data to unauthorized data brokers;

(B) "pretexting", whereby a data broker or other person represents that they are an authorized consumer and convinces an agent of the telephone company to release the data; or

(C) gaining unauthorized Internet access to account data by improperly activating a consumer's account management features on a phone company's webpage or contracting with an Internet-based data broker who trafficks in such records; and

(5) the unauthorized disclosure of telephone records not only assaults individual privacy but, in some instances, may further acts of domestic violence or stalking, compromise the personal safety of law enforcement officers, their families, victims of crime, witnesses, or confidential informants, and undermine the integrity of law enforcement investigations.

### SEC. 3. FRAUD AND RELATED ACTIVITY IN CONNECTION WITH OBTAINING CONFIDENTIAL PHONE RECORDS INFORMATION OF A COVERED ENTITY.

(a) OFFENSE.—Chapter 47 of title 18, United States Code, is amended by inserting after section 1038 the following:

#### "§ 1039. Fraud and related activity in connection with obtaining confidential phone records information of a covered entity

"(a) CRIMINAL VIOLATION.—Whoever, in interstate or foreign commerce, knowingly and intentionally obtains, or attempts to obtain, confidential phone records information of a covered entity, by—

"(1) making false or fraudulent statements or representations to an employee of a covered entity;

"(2) making such false or fraudulent statements or representations to a customer of a covered entity;

"(3) providing a document to a covered entity knowing that such document is false or fraudulent; or

"(4) accessing customer accounts of a covered entity via the Internet, or by means of conduct that violates section 1030 of this title, without prior authorization from the customer to whom such confidential phone records information relates;

shall be fined under this title, imprisoned for not more than 10 years, or both.

"(b) PROHIBITION ON SALE OR TRANSFER OF CONFIDENTIAL PHONE RECORDS INFORMATION.—

"(1) Except as otherwise permitted by applicable law, whoever, in interstate or foreign commerce, knowingly and intentionally sells or transfers, or attempts to sell or transfer, confidential phone records information of a covered entity, without prior authorization from the customer to whom such confidential phone records information relates, or knowing or having reason to know such information was obtained fraudulently, shall be fined under this title, imprisoned not more than 10 years, or both.

"(2) For purposes of this subsection, the exceptions specified in section 222(d) of the Communications Act of 1934 shall apply for the use of confidential phone records information by any covered entity, as defined in subsection (h).

"(c) PROHIBITION ON PURCHASE OR RECEIPT OF CONFIDENTIAL PHONE RECORDS INFORMATION.—

"(1) Except as otherwise permitted by applicable law, whoever, in interstate or foreign commerce, knowingly and intentionally purchases or receives, or attempts to purchase or receive, confidential phone records information of a covered entity, without prior authorization from the customer to whom such confidential phone records information relates, or knowing or having reason to know such information was obtained fraudulently, shall be fined under this title, imprisoned not more than 10 years, or both.

"(2) For purposes of this subsection, the exceptions specified in section 222(d) of the Communications Act of 1934 shall apply for the use of confidential phone records information by any covered entity, as defined in subsection (h).

"(d) ENHANCED PENALTIES FOR AGGRAVATED CASES.—Whoever violates, or attempts to violate, subsection (a), (b), or (c) while violating another law of the United States or as part of a pattern of any illegal activity involving more than \$100,000, or more than 50 customers of a covered entity, in a 12-month period shall, in addition to the penalties provided for in such subsection, be fined twice the amount provided in subsection (b)(3) or (c)(3) (as the case may be) of section 3571 of this title, imprisoned for not more than 5 years, or both.

"(e) ENHANCED PENALTIES FOR USE OF INFORMATION IN FURTHERANCE OF CERTAIN CRIMINAL OFFENSES.—

"(1) Whoever, violates, or attempts to violate, subsection (a), (b), or (c) knowing that such information may be used in furtherance of, or with the intent to commit, an offense described in section 2261, 2261A, 2262, or any other crime of violence shall, in addition to the penalties provided for in such subsection, be fined under this title and imprisoned not more than 5 years.

"(2) Whoever, violates, or attempts to violate, subsection (a), (b), or (c) knowing that such information may be used in furtherance of, or with the intent to commit, an offense under section 111, 115, 1114, 1503, 1512, 1513, or to intimidate, threaten, harass, injure, or kill any Federal, State, or local law enforcement officer shall, in addition to the penalties provided for in such subsection, be fined under this title and imprisoned not more than 5 years.

"(f) EXTRATERRITORIAL JURISDICTION.—There is extraterritorial jurisdiction over an offense under this section.

"(g) NONAPPLICABILITY TO LAW ENFORCEMENT AGENCIES.—This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or political subdivision of a State, or of an intelligence agency of the United States.

"(h) DEFINITIONS.—In this section:

"(1) CONFIDENTIAL PHONE RECORDS INFORMATION.—The term 'confidential phone records information' means information that—

"(A) relates to the quantity, technical configuration, type, destination, location, or amount of use of a service offered by a covered entity, subscribed to by any customer of that covered entity, and kept by or on behalf of that covered entity solely by virtue of the relationship between that covered entity and the customer;

"(B) is made available to a covered entity by a customer solely by virtue of the relationship between that covered entity and the customer; or

"(C) is contained in any bill, itemization, or account statement provided to a customer by or on behalf of a covered entity solely by virtue of the relationship between that covered entity and the customer.

"(2) COVERED ENTITY.—The term 'covered entity'—

"(A) has the same meaning given the term 'telecommunications carrier' in section 3 of the Communications Act of 1934 (47 U.S.C. 153); and

"(B) includes any provider of IP-enabled voice service.

"(3) CUSTOMER.—The term 'customer' means, with respect to a covered entity, any individual, partnership, association, joint stock company, trust, or corporation, or authorized representative of such customer, to whom the covered entity provides a product or service.

“(4) IP-ENABLED VOICE SERVICE.—The term ‘IP-enabled voice service’ means the provision of real-time voice communications offered to the public, or such class of users as to be effectively available to the public, transmitted through customer premises equipment using TCP/IP protocol, or a successor protocol, (whether part of a bundle of services or separately) with interconnection capability such that the service can originate traffic to, or terminate traffic from, the public switched telephone network, or a successor network.”.

(b) CHAPTER ANALYSIS.—The table of sections for chapter 47 of title 18, United States Code, is amended by adding after the item relating to section 1038 the following:

“1039. Fraud related activity in connection with obtaining confidential phone records information of a covered entity.”.

#### SEC. 4. SENTENCING GUIDELINES.

(a) REVIEW AND AMENDMENT.—Not later than 180 days after the date of enactment of this Act, the United States Sentencing Commission, pursuant to its authority under section 994 of title 28, United States Code, and in accordance with this section, shall review and, if appropriate, amend the Federal sentencing guidelines and policy statements applicable to persons convicted of any offense under section 1039 of title 18, United States Code.

(b) AUTHORIZATION.—The United States Sentencing Commission may amend the Federal sentencing guidelines in accordance with the procedures set forth in section 21(a) of the Sentencing Act of 1987 (28 U.S.C. 994 note) as though the authority under that section had not expired.

The SPEAKER pro tempore. Pursuant to the rule, the gentleman from Wisconsin (Mr. SENSENBRENNER) and the gentleman from Michigan (Mr. CONYERS) each will control 20 minutes.

The Chair recognizes the gentleman from Wisconsin.

#### GENERAL LEAVE

Mr. SENSENBRENNER. Madam Speaker, I ask unanimous consent that all Members may have 5 legislative days within which to revise and extend their remarks and include extraneous material on H.R. 4709 currently under consideration.

The SPEAKER pro tempore. Is there objection to the request of the gentleman from Wisconsin?

There was no objection.

Mr. SENSENBRENNER. Madam Speaker, I yield myself such time as I may consume.

Madam Speaker, I rise in support of H.R. 4709, the Law Enforcement and Phone Privacy Protection Act of 2006. This legislation will protect the privacy of consumers' cell phone records and create new criminal penalties for the unauthorized purchase, sale or disclosure of such records.

Certain unscrupulous companies operating on the Internet use deception to acquire an individual's phone records and then sell this personal information. Typically these companies employ a tactic known as “pretexting” to deceive the phone companies.

□ 1445

By impersonating the actual cell phone account holder, these companies are often able to obtain significant private information about the individuals.

This practice not only presents a threat to the privacy of the average consumer; the Judiciary Committee has also learned that criminals have employed these services to determine the identity of undercover law enforcement officers as well as suspected confidential informants and witnesses. Additionally, stalkers and domestic users can use such information to track a victim's location and associates.

Amazingly, none of this is clearly illegal under Federal law. H.R. 4709 targets pretexting and other deceptive practices not adequately addressed by the current law and provides express protection in the criminal code for the privacy of confidential phone records information. These important new consumer protections cover the records and calling logs of cellular, land line, Voice-Over-Internet-Protocol users, and accomplish this goal on a technology neutral basis. The bill also establishes specific criminal penalties for the fraudulent acquisition or disclosure of such records without the consent of the consumer.

More specifically, the bill prohibits third parties from purchasing or receiving confidential phone records information without the prior authorization of the consumer, or knowing or having reason to know that the information was obtained fraudulently. It exempts use of information by any covered entity if such use would be permissible under existing laws governing the handling of such information by telecommunications carriers. This exception includes any uses by agents, contractors, or joint venture partners to receive the confidential phone records acting on behalf of the covered entity to perform any of the functions permitted under existing law.

The bill also provides enhanced criminal penalties for anyone who engages in large scale operations to violate the law, or who discloses or uses fraudulently obtained confidential phone records information in furtherance of crimes of violence, including domestic violence and stalking, or to kill, injure or intimidate a witness, juror, confidential informant, or law enforcement officer.

The bill under consideration today incorporates several technical and conforming changes to the text that was reported unanimously by the Judiciary Committee on March 2 this year. This bipartisan legislation is supported by the U.S. Department of Justice, the National Center For Victims of Crime, the Cellular Telecommunications and Internet Association, and all of the major land line and mobile telephone companies.

I commend the chairman of the Subcommittee on Courts, the Internet, and Intellectual Property, Lamar Smith, for introducing this important measure. I also want to thank Judiciary Committee Ranking Member CONYERS, Congressman GOODLATTE, and Congressman SCOTT for their contributions to this legislation.

Madam Speaker, H.R. 4709 provides consumers with important new protections for the confidentiality of their calling records without compromising the legitimate lawful interests of law enforcement, emergency services and cellular telephone service providers. I urge my colleagues to support this sensible piece of legislation and hope that the Members of the other body will consider and pass this bill expeditiously.

Madam Speaker, I reserve the balance of my time.

The SPEAKER pro tempore (Mrs. DRAKE). Without objection, the 20 minutes will be controlled by the gentlewoman from Texas (Ms. JACKSON-LEE).

There was no objection.

Ms. JACKSON-LEE of Texas. Madam Speaker, I yield myself such time as I may consume.

I rise with great pleasure and enthusiasm as one of the supporters of this legislation, Telephone Records and Privacy Protection Act of 2006, H.R. 4709; and I am pleased to acknowledge Mr. LAMAR SMITH and JOHN CONYERS as the original sponsors of this legislation.

I thank the chairman for yielding me this time, and I add my applause to legislation that makes several important and noteworthy changes to current law.

First and foremost, it establishes a new criminal offense against anyone who knowingly and intentionally obtains or attempts to obtain the confidential phone records of a third party through any one of the bill's several enumerated schemes or devices to defraud. Penalties for violating this prohibition include a fine or a term of imprisonment of not more than 20 years, or both.

Second, the bill establishes a new set of criminal penalties for anyone who knowingly and intentionally sells or purchases the confidential phone records of a third party without proper authorization or knowing that such records were obtained through fraud. Violators of either of these two provisions are subjected to a maximum term of imprisonment of up to 5 years.

Finally, in an effort to offer increased protection to the likely victims of such activities, this legislation includes a series of enhanced criminal penalties against any individual who engages in any one of the aforementioned crimes knowing that such information was sought in furtherance of or with the intent to commit any one of the bill's dozen or so enumerated offenses. Individuals specifically protected under this provision include potential victims of domestic-violence-related offenses, jurors, criminal witnesses, confidential informants, and law enforcement officers.

Recent investigations undertaken by State and Federal law enforcement officials have demonstrated the ease with which an individual can obtain the confidential calling records of a third party. By simply contacting one of the

many on-line data brokers that currently exist, the private records of anyone sitting in this room could be filtered into the public domain within a matter of minutes.

And if put into the wrong hands, such information could be used to commit countless crimes of violence, including acts of domestic violence, retaliatory acts against law enforcement officers, or acts aimed at undermining our current criminal justice system.

Madam Speaker, I think it is important to note that as we fight the crime of identity theft, this new and innovative legislation puts a dagger in some aspects of that. For example, the records of high-ranking officials dealing with government business could be secured, whether it is local, State or Federal, and put various actions of the government in jeopardy.

And, yes, a law enforcement officer that may be undercover, those records can be secured and immediately put that law enforcement officer in great jeopardy of his or her life.

And, finally, for those of us who are parents, we understand what it means to be able to communicate with a young person through a cell phone. Just imagine a stalker or a child predator securing those records of your teenage son or daughter. What a horrific thought to think.

And so it is important that this legislation be passed for the protection of Americans all over this country and as well for the integrity of our technology system.

The bill before us seeks to stop these potential abuses from becoming a reality, and I strongly urge my colleagues to support this worthwhile measure.

I am pleased to acknowledge LAMAR SMITH and JOHN CONYERS as the original sponsors of this bill. This legislation makes several important and noteworthy changes to current law.

First and foremost, it establishes a new criminal offense against anyone who knowingly and intentionally obtains, or attempts to obtain, the confidential phone records of a third party through any one of the bill's several enumerated schemes or devices to defraud. Penalties for violating this prohibition include a fine or a term of imprisonment of not more than 20 years, or both.

Second, the bill establishes a new set of criminal penalties for anyone who knowingly and intentionally sells or purchases the confidential phone records of a third party, without proper authorization or knowing that such records were obtained through fraud. Violators of either of these two provisions are subjected to a maximum term of imprisonment of up to 5 years.

Finally, in an effort to offer increased protection to the likely victims of such activities, the legislation includes a series of enhanced criminal penalties against any individual who engages in any one of the aforementioned crimes knowing that such information was sought in furtherance of, or with the intent to commit any one of the bill's dozen or so enumerated offenses. Individuals specifically protected under this provision include potential victims of domestic-violence related offenses,

jurors, criminal witnesses, confidential informants and law enforcement officers.

Recent investigations that have been undertaken by State and Federal law enforcement officials have demonstrated the ease with which an individual can obtain the confidential calling records of a third party. By simply contacting one of the many online data brokers that currently exist, the private records of anyone sitting in this room could be filtered into the public domain within a matter of minutes.

And, if put into the wrong hands, such information could be used to commit countless crimes of violence, including acts of domestic violence, retaliatory attacks against law enforcement officers, or acts aimed at undermining our current criminal justice system.

The bill before us seeks to stop these potential abuses from becoming a reality. I strongly urge my colleagues to support this worthwhile measure.

Madam Speaker, I reserve the balance of my time.

Mr. SENSENBRENNER. Madam Speaker, I yield such time as he may consume to the gentleman from Texas (Mr. SMITH), the author of the bill.

Mr. SMITH of Texas. Madam Speaker, since I introduced this legislation, I rise in strong support of the Telephone Records and Privacy Protection Act of 2006, the TRAPP Act. And I want to thank Chairman SENSENBRENNER for his leadership and continuing support of this bicameral and bipartisan bill.

Madam Speaker, few things are more personal and potentially more revealing than our telephone records. Who we call can reveal much about our business and personal lives, including intimate details about one's medical or financial condition. Calling records can even be used to identify a caller's location. In some cases the unauthorized release of personal information like a phone record can lead to a tragic result.

Unfortunately, existing Federal statutes that could be used to target data thieves are inadequate. These statutes have clearly not deterred data burglars from treating confidential phone record information as a commodity to be bought and sold over the Internet without the consent of consumers, sometimes for as little as \$100.

The underlying bill targets companies and individuals who traffic in fraudulently obtained confidential phone records and provides new protections for the privacy of calling logs themselves. It establishes a new section, 1039, in title 18 of the United States Code, that will provide explicit penalties for those who use fraud to obtain confidential phone records.

Madam Speaker, the bill imposes a prison sentence of up to 10 years and a fine of up to \$500,000 on any person who, in interstate commerce, sells, transfers, purchases or receives confidential phone records of a telephone company without the prior consent of the consumer.

The bill includes enhanced penalties for cases where the information is used in furtherance of crimes of domestic violence or a threat to law enforcement officials or their families.

We need to pass this bill to demonstrate that we take seriously the obligation to protect the confidentiality of consumer telephone records and to make clear to data thieves that their conduct will result in a felony conviction.

This legislation supports crime victims, prosecutors, and companies and individuals who have been the targets of this fraud. A companion measure is expected to be introduced soon in the Senate.

Madam Speaker, I urge my colleagues to support this legislation.

Mr. SENSENBRENNER. Madam Speaker, at this time I have no further speakers, and I am prepared to yield back if the gentlewoman from Texas will yield back.

Ms. JACKSON-LEE of Texas. Madam Speaker, I include the following letters of support for this legislation:

CONSUMERS UNION,

Washington, DC., February 8, 2006.

Hon. CHARLES SCHUMER,

U.S. Senate,

Washington, DC.

Hon. ARLEN SPECTER,

U.S. Senate,

Washington, DC.

Hon. BILL NELSON

U.S. Senate,

Washington, DC.

DEAR SENATORS SCHUMER, SPECTER AND NELSON: Consumers Union, the publisher of Consumer Reports, supports the Consumer Telephone Records Protection Act of 2006, S. 2178, and applauds your leadership on this critical consumer issue.

The Consumer Telephone Records Protection Act would go far in protecting consumers' private telephone records. Consumers have a reasonable expectation that their calling records will not be released to anyone other than themselves. Congress must meet that expectation by preventing stalkers, identity thieves, and shady data-brokers from accessing consumers' personal telephone calling records. Subjecting to criminal penalties the selling of those records and the practice of pretexting to obtain them will serve as a strong deterrence.

Importantly, instead of simply reaffirming Federal Trade Commission authority to enforce penalties against unfair and deceptive trade practices, the Consumer Telephone Records Protection Act ensures that other federal entities are empowered to protect consumers' calling records. Additionally, the bill covers all wireline, wireless and VoIP services, protecting the rights of consumers to keep their phoning records private regardless of which platform they use.

We look forward to working with you toward adoption of S. 2178 as well as other complementary measures required to protect consumers phone records. These include stronger enforcement powers and penalties for FTC and the Federal Communications Commission; mandatory consumer notice when calling records have been requested or provided to any party; requirements that consumers affirmatively opt-in before any of their records are shared, even with affiliates of the phone company; and finally, provisions strengthening carrier internal processes for safeguarding consumer information under Section 222 of the 1934 Communications Act, with tough penalties for non-compliance.

We applaud your swift action and thank you for your leadership to protect consumers. We look forward to working with you toward effective, enforceable consumer phone record privacy legislation.

We look forward to working with you toward enactment of this important legislation.

Respectfully,

JEANNINE KENNEY,  
Senior Policy Analyst.

VERIZON WIRELESS APPLAUDS CELL PHONE  
PRIVACY BILL

BEDMINSTER, NJ.—Senators Charles Schumer of New York, Arlen Specter of Pennsylvania and Bill Nelson of Florida proposed legislation in the U.S. Senate today to make it a crime for someone to obtain cell phone customer calling or billing information under false pretenses or for a wireless company employee to sell such customer information. Verizon Wireless issued the following statement from Steve Zipperstein, vice president of legal & external affairs, in response to the filing:

"As the first wireless company in the U.S. to take legal action to protect cell phone customers' private account information from so-called online data brokers, Verizon Wireless applauds the efforts of Senators Schumer, Specter and Nelson to protect our customers' privacy from the crooks and predators who we've been hauling into civil court. The criminal penalties in this bill will provide another powerful weapon in the legal arsenal that the private sector and the government can use to protect consumers. We believe this legislation will give federal prosecutors and others in law enforcement the tools they need to crack down on this despicable practice and help defend the privacy of U.S. cell phone customers."

Verizon Wireless' record of aggressively protecting customer privacy has put the company at the forefront of the U.S. wireless industry.

On September 15, 2005, Verizon Wireless secured a permanent injunction against Source Resources Inc., a Tennessee-based company, to halt its illegal practice of obtaining and selling confidential customer telephone records. Verizon Wireless brought the lawsuit, believed to be the first of its kind, after one of its customers reported that his confidential wireless phone records had been secured without his permission by Source Resources. <http://news.vzw.com/news/2005/09/pr2005-09-15.html>

On November 9, 2005, Verizon Wireless obtained an immediate injunction against Global Information Group (GIG) of Temple Terrace, FL after the company made "thousands of attempts" to gather confidential information without proper authorization and used various fraudulent "schemes" to do so, including impersonating Verizon Wireless employees and posing as Verizon Wireless customers. The suit is pending. <http://news.vzw.com/news/2005/11/pr2005-11-09a.html>

In other actions to protect customer privacy: Verizon Wireless won permanent injunctions to stop two telemarketing firms—Intelligent Alternatives of San Diego, CA, and Resort Marketing Trends of Coral Springs, FL—from making calls to Verizon Wireless customers by using auto-dialers and recorded messages. Federal consumer protection law prohibits use of auto-dialers or pre-recorded messages in calls to cell phones—<http://news.vzw.com/news/2005/12/pr2005-12-09.html>

Verizon Wireless filed a lawsuit seeking an injunction against Passport Holidays of Ormond Beach, FL for violating federal and state laws after it sent more than 98,000 unsolicited short text messages to Verizon Wireless customers informing them they supposedly had won a cruise to the Bahamas and asking them to call to claim their prize—<http://news.vzw.com/news/2005/11/pr2005-11-23.html>

In August 2004, Verizon Wireless obtained an injunction against Rhode Island resident Jacob Brown, a known spammer who had been sending numerous text message solicitations to Verizon Wireless customers—<http://news.vzw.com/news/2004/08/pr2004-08-30.html>

In June 2004, Verizon Wireless broke with the wireless industry by becoming the first to announce it would protect customer privacy by refusing to participate in a national wireless phone directory—<http://news.vzw.com/news/2004/06/pr2004-06-21.html>

SPRINT NEXTEL SUES TO SHUT DOWN ONLINE  
SERVICES THAT ILLEGALLY OBTAIN AND  
SELL CONFIDENTIAL TELEPHONE RECORDS

RESTON, VA.—(Business Wire)—Jan. 27, 2006—Sprint Nextel Corp. (NYSE:S) announced today that it has filed a lawsuit against the parent company of four online data brokers that use illegal and deceptive practices to obtain and sell wireless customer call detail records. Sprint Nextel states within the Complaint that 1st Source Information Specialists Inc., parent company of [www.locatecell.com](http://www.locatecell.com), [www.celltolls.com](http://www.celltolls.com), [www.datafind.org](http://www.datafind.org) and [www.peoplesearchamerica.com](http://www.peoplesearchamerica.com), employs fraudulent tactics, such as posing as customers seeking information about their own accounts, to access cell phone logs and phone numbers.

In the suit filed today in Florida, Sprint Nextel states that the schemes conducted by these fraudulent online services invade the privacy of Sprint Nextel's customers. Sprint Nextel has requested both temporary and permanent injunctions against 1st Source Information Specialists Inc.

"Protection of confidential customer information is our number one priority and we are taking aggressive action to ensure that any threat to privacy is eliminated immediately," said Kent Nakamura, vice president for telecom management and chief privacy officer for Sprint Nextel. "1st Source Information Specialists continues to display egregious disregard for privacy, and previous industry-driven actions do not appear to have deterred their illegal activities. We can assure our customers that we will make every effort to put these services out of business."

To further demonstrate its commitment to protecting consumer privacy, Sprint Nextel is supporting federal legislation that seeks to increase criminal and/or civil penalties against third party companies that fraudulently seek to obtain, sell or distribute customer records. In particular, Sprint Nextel hails legislation crafted by senators Charles Schumer of New York, Arlen Specter of Pennsylvania and Bill Nelson of Florida for its provisions that make it illegal to obtain telephone customer records, and that stiffen prison sentences and fines for those companies fraudulently selling information. Sprint Nextel looks forward to working with these senators and other members of Congress to pass the legislation that best protects consumers and ends this fraudulent practice.

In addition to launching a legal assault on these illegal activities, Sprint Nextel's corporate security and customer care teams employ safeguards to protect confidential customer information from unauthorized access. Sprint Nextel customer service agents have been made aware of the fraudulent tactics used by online data brokers, and they are trained to follow detailed authentication procedures when responding to customer inquiries. Sprint Nextel's security practices were validated in 2005 when the company was awarded the "Best Practice in Security for Governance" by the Aberdeen Group.

Sprint Nextel strongly encourages its customers to take precautions to protect them-

selves. In particular, Sprint Nextel recommends that customers regularly change passwords used to access account information on the Sprint.com web site or when calling customer care, and select unique passwords to access voicemail messages on Sprint phones. For additional customer privacy tips, please go to [www.sprint.com/privacy](http://www.sprint.com/privacy).

COUNTY OF LOS ANGELES,

Monterey Park, CA, March 29, 2006.

Hon. CHARLES SCHUMER,  
U.S. Senate,  
Washington, DC.

UNITED STATES SENATE BILL 2178—SUPPORT  
CONSUMER TELEPHONE RECORDS PROTECTION  
ACT OF 2006 AS INTRODUCED ON JANUARY 18,  
2006

DEAR SENATOR SCHUMER: The Los Angeles County Sheriff's Department is proud to support your United States Senate Bill 2178 (S. 2178). This Bill would prohibit the obtaining, by fraud or other unauthorized means, of confidential phone record information.

Recently, there has been a lot of media focus regarding the sale of another's cell phone records over the internet. Many companies, charging as little as \$20, offer to research and provide a month's worth of cell phone call information, no questions asked.

With the above in mind, S. 2178 seeks to correct this serious situation by prohibiting another from obtaining this information under false pretense or selling such information by any person, including an employee of the provider.

As Sheriff of Los Angeles County, I support S. 2178. Should you need further assistance regarding this issue please do not hesitate to contact me directly at (323) 526-5000, or my Legislative Advocate, Sergeant Wayne Bilowit, at (323) 240-5696.

Sincerely,

LEROY D. BACA,  
Sheriff

T-MOBILE SUES CELL RECORD BROKERS FOR  
CRIMINAL PROFITTEERING

BELLEUE, WA., January 23, 2006—In an effort to restrain the unlawful activities of entities that attempt to fraudulently obtain confidential customer information, T-Mobile USA, Inc. is bringing legal action against online data brokers the company believes are involved in illegitimately obtaining and selling call records. Acting under Washington State criminal profiteering laws, T-Mobile today filed suit in King County, Wash., Superior Court seeking an injunction to stop [Locatecell.com](http://Locatecell.com), as well as related companies and individuals, from engaging in such illegal behavior. T-Mobile also is prepared to take similar legal action against other believed violators.

"To further safeguard the privacy of our customers, T-Mobile is taking action to prosecute these online data brokers to the fullest extent permitted by the law," said Dave Miller, Senior Vice President and General Counsel, T-Mobile USA. "For the protection of all wireless customers, their illegal actions must be stopped."

T-Mobile also endorses the need for federal legislation making it a crime for anyone to obtain, sell or distribute, through fraudulent means, the private calling records of mobile phone customers.

"T-Mobile supports adoption of federal legislation making it clear that fraudulent activities by third parties to obtain, sell, or distribute call records is a crime," said Tom Sugrue, T-Mobile's Vice President of Government Affairs. "Legislation should address the deplorable and deceptive actions of these third-party brokers who illegitimately obtain and sell call records without the knowledge or consent of wireless customers. We

applaud the FCC's recent citations against brokers that have defied its subpoenas."

Legislation introduced by Sens. Schumer, Specter and Nelson and co-sponsored by Sens. Burns and Reid, takes particular aim at these perpetrators, defined as anyone who sells or obtains confidential customer information through deception or unauthorized access to a telephone company's data. T-Mobile commends this bipartisan group of Senators for targeting privacy predators such as online brokers in an effort to bolster protections for consumers. T-Mobile looks forward to working with members of Congress to resolve this important privacy concern.

As a result of data uncovered during a continuing, thorough internal investigation, T-Mobile had issued numerous cease and desist letters against companies that were believed to have illegally obtained and sold phone-calling records of some of its customers.

T-Mobile reiterates that it is important for customers to continue to take steps to protect their accounts by utilizing passwords. T-Mobile urges all users of mobile phone services to take the following password protection steps:

Create separate passwords for voicemail, online access, and for use when calling customer care about your billing account.

Set complex passwords using both numbers and letters where appropriate.

Avoid common passwords such as birth dates, family or pet names and street addresses.

Change your passwords at least every 60 days.

Memorize your passwords.

Don't share passwords with anyone.

"T-Mobile takes customer privacy seriously. Customer protection is a primary concern. We have invested millions of dollars to help protect customer information, and we continue to further reinforce our systems. Our customer phone records are not for sale," said Sugrue. "We encourage Congress and the FCC to act swiftly to bring the illegal activity of online data brokers to an end."

Mr. SMITH of Texas. Madam Speaker, since I introduced this legislation, I rise in strong support of the "Telephone Records and Privacy Protection Act of 2006 (the TRAPP Act)."

And I want to thank Chairman SENSENBRENNER for his leadership and continuing support of this bicameral and bipartisan bill.

Madam Speaker, few things are more personal and potentially more revealing than our phone records.

Who we call can reveal much about our business and personal lives, including intimate details about one's medical or financial condition.

Calling records can even be used to identify a caller's location.

In some cases, the unauthorized release of personal information like a phone record can lead to a tragic result.

Unfortunately, existing Federal statutes that could be used to target data thieves are inadequate.

These statutes have clearly not deterred data burglars from treating confidential phone records information as a commodity, to be bought and sold on the Internet, without the consent of consumers, for about \$100.

The underlying bill targets companies and individuals who traffic in fraudulently obtained confidential phone records and provides new protections for the privacy of calling logs.

It establishes a new section 1039 in Title 18 of the United States Code that will provide explicit penalties for those who use fraud to obtain confidential phone records.

The bill imposes a prison sentence of up to 10 years and a fine of up to \$500,000 on any person who in interstate commerce sells, transfers, purchases or receives confidential phone records of a telephone company without the prior consent of the customer.

The bill includes enhanced penalties for cases where the information is used in furtherance of crimes of domestic violence or threat to law enforcement officers or their families.

We need to pass this bill to demonstrate that we take seriously the obligation to protect the confidentiality of consumer telephone records and to make clear to data thieves that their conduct will result in a felony conviction.

This legislation supports crime victims, prosecutors, and companies and individuals who have been the targets of this fraud.

A companion measure is expected to be introduced soon in the Senate.

Mr. GOODLATTE. Madam Speaker, I rise in strong support of H.R. 4709, the Law Enforcement and Phone Privacy Protection Act. I was pleased to join with Representatives SMITH, CONYERS and SCOTT to introduce this important legislation to protect phone records from thieves and opportunists.

The sale of confidential phone records is a serious problem. For approximately \$100, anyone can buy an individual's private cell phone call history. These histories catalogue every outgoing and incoming call a customer makes or receives. This information should not be available for unauthorized sale on the Internet.

The primary method thieves use to obtain this information is known as "pretexting". This involves an individual with some key information—a cell phone number or possibly a Social Security Number—pretending to be the subscriber to get information about an account. The Law Enforcement and Phone Privacy Protection Act puts a stop to this by imposing criminal penalties for "pretexting." As well as other methods of seeking to obtain such records through the use of fraud.

Furthermore, this legislation will provide additional punishment for those who illegally sell or obtain phone records knowing they will be used in a criminal act. This is extremely important for the protection of law enforcement officers and potential victims of domestic violence, whose call histories may be particularly desirable to those who wish to do them harm.

We all use telephones and cell phones with the assumption that information about who we receive calls from and make calls to will not fall into the wrong hands. I urge the members of the house to support this legislation to ensure that phone records are protected.

Mr. CANTOR. Madam Speaker, I rise today in support of the Law Enforcement and Phone Privacy Protection Act of 2006.

As America continues to prosper, cell phones are becoming increasingly central to our everyday lives. We use this technology to keep in closer contact with our families, manage our livelihoods, and stay in touch with friends. We trust that the records of private conversations remain safe. Law enforcement must have the tools necessary to ensure the privacy of our cell phone records and prosecute those who invade our lives.

Today, criminals can use our cell phone records to expose a government informant, steal our personal information, or commit other forms of fraud.

This bill takes strong action to protect the privacy of American's cell phone records. By providing tough new protections, we can better ensure the privacy of confidential cell phone records. Law enforcement and prosecutors can impose serious criminal penalties on those who unlawfully invade and use our cell phone records.

Congress has a duty to protect all Americans and their confidential cell phone records.

Ms. ZOE LOFGREN of California. Madam Speaker, I am pleased to be an original co-sponsor of this bill. I believe it provides critical privacy protections to the more than 180 million Americans who use cell phones. It will also protect the privacy of more than 100 million American homes with wired telephones. And it will protect Voice over IP users, now more than 2 million Americans and rapidly rising.

I think we've heard too many stories of how easy it is to fraudulently obtain cell phone call records and even cell phone locations. We've heard of how one political blog bought Wesley Clark's cell phone records, but the fact is lots of ordinary Americans have reason to be concerned about the privacy of their phone records. Imagine what a criminal organization could do with the cell phone call records of an undercover law enforcement agent, or what an abuser could do with a spouse's cell phone location. No one should be able to get another person's phone records through fraud, and this bill makes it a crime to purchase or use phone records obtained through fraud.

I want to thank Chairman SMITH of the Intellectual Property Subcommittee and Ranking Member CONYERS of the Judiciary Committee for their leadership in drafting this legislation, which I believe represents a sensible, bipartisan solution to a growing problem. I urge my colleagues to join me in voting to pass this bill.

Ms. JACKSON-LEE of Texas. Madam Speaker, I ask the support of this legislation, and I yield back the balance of my time.

Mr. SENSENBRENNER. Madam Speaker, I yield back the balance of my time.

The SPEAKER pro tempore. The question is on the motion offered by the gentleman from Wisconsin (Mr. SENSENBRENNER) that the House suspend the rules and pass the bill, H.R. 4709, as amended.

The question was taken.

The SPEAKER pro tempore. In the opinion of the Chair, two-thirds of those present have voted in the affirmative.

Mr. SENSENBRENNER. Madam Speaker, on that I demand the yeas and nays.

The yeas and nays were ordered.

The SPEAKER pro tempore. Pursuant to clause 8 of rule XX and the Chair's prior announcement, further proceedings on this question will be postponed.

# SUPPORTING THE GOALS AND IDEALS OF NATIONAL CYSTIC FIBROSIS AWARENESS MONTH

Mr. STEARNS. Madam Speaker, I move to suspend the rules and agree to the concurrent resolution (H. Con. Res. 357) supporting the goals and ideals of National Cystic Fibrosis Awareness Month.

The Clerk read as follows:

H. CON. RES. 357

Whereas cystic fibrosis is one of the most common life-threatening genetic diseases in the United States and one for which there is no known cure;

Whereas the average life expectancy of an individual with cystic fibrosis is 35 years, an improvement from a life expectancy of 10 years in the 1960s, but still unacceptably short;

Whereas approximately 30,000 people in the United States have cystic fibrosis, more than half of them children;

Whereas one of every 3,500 babies born in the United States is born with cystic fibrosis;

Whereas more than 10,000,000 Americans are unknowing, symptom-free carriers of the cystic fibrosis gene;

Whereas the Centers for Disease Control and Prevention recommends that all States consider newborn screening for cystic fibrosis;

Whereas the Cystic Fibrosis Foundation urges all States to implement newborn screening for cystic fibrosis to facilitate early diagnosis and treatment which improves health and longevity;

Whereas prompt, aggressive treatment of the symptoms of cystic fibrosis can extend the lives of people who have the disease;

Whereas recent advances in cystic fibrosis research have produced promising leads in gene, protein, and drug therapies beneficial to people who have the disease;

Whereas innovative research is progressing faster and is being conducted more aggressively than ever before, due, in part, to the Cystic Fibrosis Foundation's establishment of a model clinical trials network;

Whereas although the Cystic Fibrosis Foundation continues to fund a research pipeline for more than two dozen potential therapies and funds a nationwide network of care centers that extend the length and quality of life for people with cystic fibrosis, lives continue to be lost to this disease every day;

Whereas education of the public about cystic fibrosis, including the symptoms of the disease, increases knowledge and understanding of cystic fibrosis and promotes early diagnosis; and

Whereas the Cystic Fibrosis Foundation will conduct activities to honor National Cystic Fibrosis Awareness Month in May, 2006: Now, therefore, be it

*Resolved by the House of Representatives (the Senate concurring), That the Congress—*

(1) honors the goals and ideals of National Cystic Fibrosis Awareness Month;

(2) promotes further public awareness and understanding of cystic fibrosis;

(3) advocates for increased support for people who have cystic fibrosis and their families;

(4) encourages early diagnosis and access to quality care for people with cystic fibrosis to improve the quality of their lives; and

(5) supports research to find a cure for cystic fibrosis by fostering an enhanced research program through a strong Federal commitment and expanded public-private partnerships.

The SPEAKER pro tempore. Pursuant to the rule, the gentleman from

Florida (Mr. STEARNS) and the gentleman from Massachusetts (Mr. MARKEY) each will control 20 minutes.

The Chair recognizes the gentleman from Florida.

## GENERAL LEAVE

Mr. STEARNS. Madam Speaker, I ask unanimous consent that all Members may have 5 legislative days within which to revise and extend their remarks and insert extraneous material on this resolution.

The SPEAKER pro tempore. Is there objection to the request of the gentleman from Florida?

There was no objection.

Mr. STEARNS. Madam Speaker, I yield myself such time as I may consume.

Madam Speaker, I rise today in support of H. Con. Res. 357, which supports the goals and ideals of National Cystic Fibrosis Awareness Month, beginning in May. Every year in the United States, about 1,000 children are born with cystic fibrosis, or CF, a life-shortening genetic disease.

According to the Cystic Fibrosis Foundation, those children face a median life expectancy of 36 years, an average that, fortunately, has continued to increase as science and research have developed better treatment and drugs. And while a median life expectancy of 36 is unacceptably low, that figure is cause for hope for those living with the disease and, of course, their families. They know that in 1955, the year parents of children suffering from this disease formed the Cystic Fibrosis Foundation, children born with CF usually did not live to attend preschool. As the life expectancy increases, those suffering with this disease and their families continue to work for a cure or a life-extending treatment.

Madam Speaker, while a cure for cystic fibrosis remains illusive, the symptoms and effects of the disease are fairly simple. CF is one of the most common life-threatening genetic diseases in the United States. More than 30,000 people in the United States have CF, and over half of them are children.

In addition, over 10 million Americans are unknowing, symptom-free carriers of the cystic fibrosis gene. Cystic fibrosis affects the lungs and digestive system.

□ 1500

The defective gene that causes CF triggers the production of abnormally thick mucus in the lungs that leads to restricted breathing, recurring lung infections, and in many cases digestive problems. The infections deteriorate the lungs and their capacity to deliver oxygen to the body, a condition that worsens over time and in many cases even leads to death or the need for a lung transplant. One of the goals of H. Con. Res. 357 is to promote the need for early diagnosis and the importance of newborn screening so that treatment of children with CF can begin as soon as possible to improve their health and longevity.

The five decades that have passed since the founding of the Cystic Fibrosis Foundation have brought not only hope but years to the lives of those suffering from CF. The Cystic Fibrosis Foundation continues to be at the forefront of making more with less in the area of drug discovery and development. The Therapeutics Development Program, TDP, created and launched by the CF Foundation, has pioneered new ways to conduct cutting-edge, life-saving research in a cost-effective and efficient manner. This program now includes 18 major research institutions across the country in an established clinical trials network. The TDP provides innovative companies with funding, raised through private donations to the CF Foundation, to undertake research and development on promising new drug candidates, and supports an extensive pipeline of potential new therapies. In fact, the CF Foundation currently has more than 30 drugs and therapies in various stages of clinical trials, any one of which could dramatically improve the life of someone suffering from CF. I believe that the innovative programs like the Therapeutics Development Program are part of the blueprint for more efficient and cost-effective health care and should be supported. So, as you can see, Madam Speaker, CF Foundation-sponsored research is adding precious years to the lives of those living with the disease so that they might live long enough to benefit once a cure is found.

Today there is more potential research on new drugs and therapies than funds to finance that lifesaving work. This is a problem created by a wealth of scientific riches, and one that I hope can be bridged by more public-private partnerships which leverage our world-class biotech and pharmaceutical companies with the capabilities of institutions like the National Institutes of Health to ensure that the discovery phase of identifying new drugs and compounds to treat cystic fibrosis continues. To that end the resolution before us today advocates strong partnerships between government resources like the NIH and nonprofits like the Cystic Fibrosis Foundation as a key means to improve care for those with "orphan" diseases like CF.

Madam Speaker, in closing, I would like to commend my friend and colleague Mr. MARKEY from Massachusetts for his leadership and work supporting this resolution and for our partnership cochairing a new Congressional Cystic Fibrosis Caucus. The Congressional Cystic Fibrosis Caucus, like this resolution, is intended to provide Members and the American public a better understanding of cystic fibrosis and the need to support the incredible work that is being done by the Cystic Fibrosis Foundation as well as through public-private collaboration to find a cure.

I would also like to thank all those Members on both sides of the aisle who have cosponsored H. Con. Res. 357 and